UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/493,031	01/28/00	SAMID G	4427-002

LM02/0601

Lowe Hauptman Gopstein Gilman & Berner L
1700 Diagonal Road Suite 310
Alexandria VA 22314

EXAMINER	
LAUFER,P	
ART UNIT	**PAPER NUMBER**
2766	3

DATE MAILED: 06/01/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
09/493,031	Gideon Samid
Examiner	**Group Art Unit**
Pinchus M. Laufer	2766

☒ Responsive to communication(s) filed on *3 Apr 2000*.

☐ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *1-16* is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *1-16* is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐approved ☐disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____.

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). *2*

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

PART III DETAILED ACTION

Claim Rejections - 35 U.S.C. § 112

1. Claims 7, 8, 11, 12, 15, and 16 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 7 and 8: The phrase "the second key" has no antecedent basis.

Claim 15: The phrase "elements of different colors" is not clear within the context of the claim.

Claim 16: The phrase "large number" is a relative term which renders the claim indefinite. The term "large number" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

For the aforementioned reasons the claims and all claims depending therefrom are indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 14 is rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

There is no disclosure as to how a single given key and ciphertext can reproduce multiple messages. What is disclosed is that a single ciphertext when paired with different keys can lead to different messages upon decryption.

Claim Rejections - 35 U.S.C. § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. § 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-16 are rejected under 35 U.S.C. § 102(a,b) as being clearly anticipated by Leonardo/Daniel (last reference on first page of IDS).. This disclosure matches the patent disclosure. As there is no identification of authorship other that D&G Sciences there is a presumption that the author is not the Applicant. The similarity of this reference to the application indicates that Applicant is best positioned to clarify the authorship and date of this article.

6. Claims 1, 4, 6, 7, 9-13 and 15-16 are rejected under 35 U.S.C. § 102(b) as being clearly anticipated by Gaines (Reference R, 1939). Gaines (pages 200-207, see particularly, 200-201 first paragraph and final paragraph on 207) describes the Playfair substitution cipher and points out that it is usually combined with a transposition cipher in order to make cryptanalysis more difficult. Playfair inserts nulls between all repeating letters to make a non-repeating plaintext it then performs the substitution as laid out on page 200. The addition of the nulls makes the ciphertext a different size from the plaintext. The keyword for generating the Playfair encryption matrix defines a "starting element" for the key. Alternatively, the starting point of the route transposition can be interpreted as the starting element. A route transposition is a particular way to traverse a grid (usually rectangular) which amounts to "bridges" linking each element in the non-repeat plaintext to its neighbors. With respect to claim 15, the key provides access to all elements, so it provides access to elements of "different colors" by default. Furthermore, assuming colors to mean letters in the alphabet, the key allows access to any of these as well. With respect to claim 16, the ciphertext can be matched to a large number of keys (just set up different matrices or transposition routes). this does not guarantee however that there will be a meaningful decipherment. If there are an odd number of characters in the message an additional character is added to insure pairs for encryption. This meets "expanding" of claim 6. The removal of the nulls corresponds to the claim 10 "collapsing" to obtain the message.

7. Claims 1, 4, 7, 9-13 and 15-16 are rejected under 35 U.S.C. § 102(b) as being clearly anticipated by Manual Of Cryptography (Ref S). See pages 93 and 94 which describe the line cipher. Inherent in the discussion is the use of an intervening letter between any doubles (or else there would be no line). There is a starting element denoted by one end of the figure, each vertex of the graph is a bridge, there is access to all elements, the directions include up, down left, right and the ciphertext once again can be matched with many potential keys.

Claim Rejections - 35 U.S.C. § 103

8. The following is a quotation of 35 U.S.C. § 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.
>
> Subject matter developed by another person, which qualifies as prior art only under subsection (f) or (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person.

9. Claims 1, 2, 4, 5, and 8 are rejected under 35 U.S.C. § 103 as being unpatentable over Schneier (Reference T, pages 227-228) as cited in the disclosure. Schneier teaches a method of generating a ciphertext which will decrypt to two different messages under two different keys. Schneier does not teach the claim 1 limitation of transforming the plaintext into non-repeating plaintext. The examiner asserts that it is well known to add in additional characters in a plaintext to help break up the natural building blocks of the plaintext language so that decryption is complicated. It would have been obvious to one of ordinary skill in the art to make the plaintext non-repeating in this manner to enhance the technique taught by Schneier. With respect to claims 4, 5, and 8 the key for the XOR is generally taken from a stream output of a pseudorandom number generator. Thus key1 and key2 will be presented as different portions of the same keystream, that is, they have different starting elements.

Information Disclosure Statement

10. The information disclosure statement contains 2 references with the date of download from the Internet and one with no date citation at all. Applicant is requested to provide date of publication or public availability for these submissions.

Information Regarding Communication with the PTO

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pinchus M. Laufer whose telephone number is (703) 306-4160. The examiner can normally be reached on weekdays from 8:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, G. O. Hayes, can be reached on (703) 305-9711. The fax phone number for this Group is (703) 308-9051.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3800.

May 26, 2000

Pinchus M. Laufer
Primary Examiner
Art Unit 2766